



Direktoratet for samfunnssikkerhet
og beredskap

Innblikk i øvelsesplanlegging

Helen.Knutsen@dsb.no

A person with their hair in a bun, wearing a grey patterned sweater, sits on a rocky cliff edge. They are looking out over a vast, scenic landscape featuring a deep fjord with a blue lake, surrounded by steep, forested mountains under a cloudy sky. The scene is captured from a high angle, emphasizing the scale of the natural environment.

«Et trygt og robust samfunn – der alle tar ansvar»

DSBs viktigste oppgave er å forebygge ulykker og kriser i samfunnet

Øvelse gjør mester





GK skal ha mottatt krav om løsepenger fra hackeren, men ønsket illustrasjon: Thomas Winje Øijord / NTB

GK har blitt løsepenger

Publisert 22.07.2021 11:44

Entreprenørselskapet GK har blitt utsatt for et personopplysninger er på avveie.

Hacket norsk helse henlegger saken

Opplysninger om 2,9 millioner nordmenn kan være på sporet. Spør tyder på at angrepet var organisert fra Kina.



HENLEGGES: PST-sjef Benedicte Bjørnland orienterte om etterforskningen i dag. Foto: Ole Berg-Rusten / NTB Scanpix

E24

Hacker-trusselen

10. mai kl. 18:01 **Dataangrep mot Norkart: 3,3 millioner kan være berørt** • Selskapet Norkart, som leverer IT-systemer for kart- og eiendomsinformasjon, er utsatt for et dataangrep i en søketjeneste. Persondata for opp mot 3,3 millioner innbyggere er på avveier.

Det er snakk om informasjon som navn, adresse og fødselsnummer. Det gjelder ikke folk på skjult adresse eller skjermede bygg.



ARTIKKEL

Dataangrep mot Norkart: 3,3 millioner kan være berørt



g statlig

angrep: – normalen

ataangrep. Men det er få som er



Hydro utsatt for cyberangrep

Hydro jobber på spreng for å fjerne viruset: - En svært alvorlig situasjon

Det er ennå uklart hvem som står bak cyberangrepet mot Hydro.

meter dyrt

Meninger

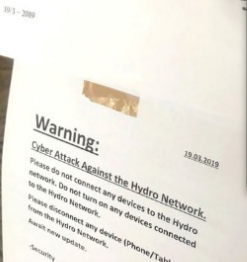


Spør om norske bedrifter vil fortsette å bli utsatt for løsepengene gjennom 2022. Foto: NTB

Trusselen er økende

ynlig at norske bedrifter vil fortsette å bli utsatt for løsepengene gjennom 2022.

Hydro er under
Cyberangrep.
Ikke koble pc til
nettverk for ny beskj



Dataangrep og hacking

OPPSUMMERT

Kinesiske og russiske hackere er mistenkt for å stå bak flere dataangrep mot norske offentlige etater og firmaer, opplyser PST. Hackerne krever i mange tilfeller løsepenger for å returnere stjalne eller låste datafiler.

16. september kl. 09:25 Politiet har klart å løse opp

Hydros «gisseldata» - I 2019 ble Hydro utsatt for et dataangrep – et løsepengenevirus.

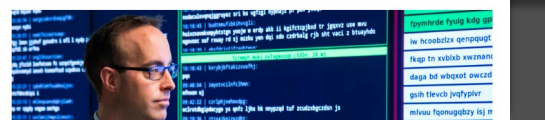
Nå har den internasjonale etterforskningen klarert krypteringsnøkler som gjør at Hydro og andre bedrifter har vært rammet kan løse opp krypteringen og dataene sine.

Det at vi har klart å finne tilbake så mange krypteringsnøkler er en stor seier for etterforskningen. sier politiet.

Russland anklages for massivt hackerangrep

- Norge opplever slike dataangrep eller forsøk på det annenhver uke

Følepleie er det uvist om Norge har blitt rammet i forbindelse med det massive dataangrepet som ble kjent mandag. Nasjonal sikkerhetsmyndighet avslører at Norge opplever lignende angrep ofte.



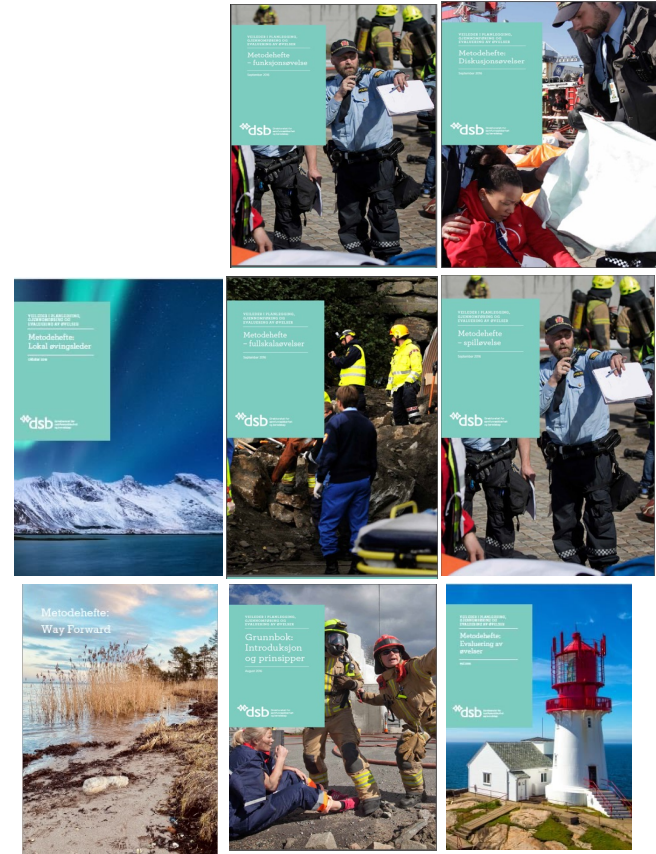
Trusler vi står ovenfor

valgmanipulasjon
skogbrann
jamming
skred
boligbrann
vulkanutbrudd
sabotasje
ekstremnedbør
flom
epidemi
strømutfall
ras
brann
legemiddel
mangel
pandemi
trusler
forsynings
sikkerhet
industribrann
nødnettutfall
solstorm
askesky
finansiell_infrastruktur
terror
tsunami
fakenews
ekstremvær

DSBs øvingsveiledere

Metodehefter:

- Grunnbok – Introduksjon og prinsipper
- Funksjonsøvelse
- Diskusjonsøvelse
- Spilløvelse
- Fullskalaøvelse
- Evaluering av øvelser
- Lokal øvingsleder
- Way forward



Grunnbok – Introduksjon og prinsipper

- Grunnboken gir en innføring i hva øvelser er, hvorfor vi øver, ulike typer øvelser og hvilke faser en øvelse består av.
- Øve for å øve
- Øve for å teste
- Øve for å lære



Funksjonsøvelser

- Funksjonsøvelser er en samlebetegnelse for øvelser som tester en eller flere funksjoner hos en aktør. Det kan gjelde teknikk, organisering eller evner.
- Funksjonsøvelser kan også omtales som prosedyreøvelser.



Funksjonsøvelser

- Sambandstester eks. Nødnett.
- Signalanlegg eks. Sivilforsvaret.
- Brannøvelser.
- Kommunikasjon, satellitt telefon, Tiger telefon etc.
- Bruk av nødaggregat.
- Tekniske installasjoner.
- Evakueringer.
- Etc.



Diskusjonsøvelse



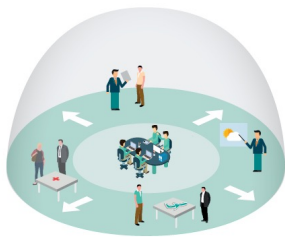
- En diskusjonsøvelse er en øvingsform der alle deltakerne samles i ett felles rom, og all kommunikasjon skjer i dette rommet.
- Innspillene blir gitt muntlig eller på papir/skjerm/lerret.
- Deltagerne skal diskutere seg gjennom problemstillinger relatert til det scenarioet de får presentert av en diskusjonsleder (øvingsleder).



Diskusjonsøvelser bidrar til:



- Øke kunnskapen om bedriftens planverk.
- Identifisere eventuell ulik forståelse og bruk av planverk.
- Identifisere ansvars- og rolleforståelse.
- Forberede kommende øvelser.
- Resonere/diskutere rundt spesielle/spørsmål.
- Diskutere risiko- og sårbarhetsanalyser og mulige hendelser som kan ramme virksomheten.



FIGUR 2. En spilløvelse kan illustreres som en «østekiokke»

Spilløvelse

- En spilløvelse kan illustreres som om spillet foregår i en "lukket boble", der de øvede aktørene befinner seg i den innerste sirkelen, og motspillet omgir dem.
- De øvede aktørene vil oftest befinne seg i sine vanlige lokaler, med de hjelpemidler de normalt har til rådighet.
- Motspillet befinner seg i andre lokaler, og styrer øvelsen ut i fra en liste med innspill (dreiebok).





Øvelsen ble en nyttig erfaring for politiet. Måne og Rønnekleiv - her på Vestbanen i Kristiansund. Foto: Erik Bliedand



Fullskalaøvelse

- Fullskala øvelser brukes ofte i forbindelse med øvelser der redningstjeneste, politi, helsevesen og Forsvaret er involvert, men kan også forekomme på andre områder.
- En fullskalaøvelse gjennomføres alltid i sanntid. Under øvelsen benyttes bekledning, arbeidsmetoder og -utstyr som man bruker til vanlig.
- Eksempler:
 - Trident Juncture 2018
 - Arctic Reihn
 - Barents rescue
 - Øvelse Nordlys



Metodehefte

Lokal øvingsleder

- Lokale øvingsledere (LØL) er "usynlige" personer som følger øvingsdeltakerne.
- Deres oppgave er å observere, vurdere, rapportere, justere, veilede og påse at sikkerheten ikke settes i fare for deltagere, innsatspersonell eller rollespillere.



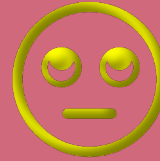
Metodehefte

Evaluering av øvelser

- Evaluering kan defineres som en systematisk vurdering i henhold til definerte mål for en øvelse og kriterier for måloppnåelse.
- Den primære hensikten med en evaluering er å muliggjøre refleksjon som kan bidra til læring og identifisering av behov for endringer.



Evaluering og læring



Hvorfor evaluere?

- Dokumentere hva som skjedde.
- Analysere.
- Vurdere.
 - Finne læringspunkter og forslag til tiltak.
- Eksempel:
 - <https://www.dsb.no/rapporter-og-evalueringer/ovelse-harbourex-2015---evaluering/>



Valg av evalueringsmetode ^{1/2}

Avhengig av hvilken type øvelse:

- Funksjonsøvelse:

- Enkel evaluering som svarer på:
- Hvilke krav stilles til oss?
- Hva fungerte/fungerte ikke?
- Kan vi bli bedre.

- Diskusjonsøvelse:

- Evalueringsnotat som løfter frem de problemstillingene som kom frem under diskusjonene.

Valg av evalueringsmetode ^{2/2}

- Spilløvelse:

Evalueringsrapport basert på:

- Spørreundersøkelser.
- Intervjuer.
- Dokumenter.
- Skjema for observasjoner.

- Fullskalaøvelse:

Evalueringsrapportens innhold:

- Formål.
- Kontekst/scenario.
- Krav.
- Vurdering av måloppnåelse.
- Anbefalinger og tiltak.

Velkommen til øvelser for bedre digital sikkerhet

Velkommen til myndighetenes øvingsportal som skal bidra til at alle virksomheter i Norge får et øvingstilbud innen digital sikkerhet. Bruk av øvelser er sentralt element i Nasjonal strategi for digital sikkerhet.

Portalen er laget som et ledd i den nasjonale øvelsen Digital 2020, og her tilbys diskusjonsøvelser basert på ulike scenarier som kan ramme din virksomhet.

Hensikten med øvelsene er at din virksomhet skal få mulighet til å diskutere seg frem til hvordan det er naturlig å håndtere ulike type hendelser. Samtidig får virksomheten din litt støtte på veien i form av diskusjonsspørsmål og råd om hva du bør tenke på for å forberede deg på denne type scenarier.

Lykke til!

Logg inn

Registrer deg



Hva er en diskusjonsøvelse? ▾

Kom i gang ▾

Forskning og diskusjonsøvelser ▾

Anbefalinger innenfor informasjonssikkerhet ▾

øvelse.no

Øvelse.no

1. Innsidere – vitende.
2. Innsidere – uvitende.
3. Kompromitterte servere.
4. Sårbarhetsvarsling.
5. Personopplysninger på avveie - forsendelse med epost.
6. Personopplysninger på avveie - phishing epost.
7. Personopplysninger på avveie – outsourchet IT-drift og bruk av Office 365.
8. Hjemmekontor.
9. Bevissthet rundt egen teknologi på reise/privat.
10. Direktørsvindel.
11. Samfunnskritiske funksjoner ute av spill - nettbanker og betalingsterminaler svikter.
12. Samfunnskritiske systemer ute av spill - strøm slås ut.



The screenshot shows the website Øvelse.no with a navigation bar at the top containing the logo, "Øvelser", "Min organisasjon", "Min profil", "Om øvelse.no", and "Logg ut". The main content area is titled "Øvelser" and lists three exercises:

- Samfunnskritiske funksjoner ute av spill**
Scenariet i denne øvelsen tar utgangspunkt i at banktransaksjoner i banken som din organisasjon benytter blir hacket med trojaner som stanser alle transaksjoner.
Sektor: Offentlig
Størrelse: 100+
[Se øvelse →](#)
- Innsider vitende**
Scenariet i denne diskusjonsøvelsen handler om hvordan en ansatt deler sensitive organisasjonsinterne opplysninger til tilfeldige nye samarbeidspartnere. Øvelsen gir grunnlag for å diskutere hvordan slike og liknende innside-trusler kan og bør håndteres.
Sektor: Offentlig
Størrelse: 100+
[Se øvelse →](#)
- Samfunnsviktige systemer ute av spill**
Scenariet i øvelsen handler om at noen av energisektorens SCADA-systemer blir satt ut av spill og hvilke konsekvenser dette får for din organisasjon. SCADA (Supervisory Control And Data Acquisition) brukes til overvåking og kontroll av infrastruktur. Det kan også være for eksempel trafikksignaler, gasslinjer, vannverk, eller lufttransport. I løpet av øvelsen kan man gjerne diskutere konsekvenser av bortfall av disse systemene også. Det er smart å ha med en som jobber med informasjonssikkerhet i øvelsen, for å få vite hva som er situasjonen i din organisasjon i dag. Dersom du ikke har en informasjonssikkerhetsansvarlig i organisasjonen, så er spørsmålene som driver øvelsen fremover (som beskrevet i info til øvingsteder) gode å ha.
Sektor: Offentlig
Størrelse: 100+
[Se øvelse →](#)

Below the list, the text "Sårbarhetsvarsling" is partially visible.

Grethe Østby

Stipendiat - [Institutt for informasjonssikkerhet og kommunikasjonsteknologi](#)

“Digital transformation of public security - developing triple-loop-learning artifacts to meet emerged information security incident response resilience and readiness challenges in public emergency organizations”

<https://www.linkedin.com/in/grethe-%C3%B8stby-aa396063/>

<https://www.ntnu.no/ansatte/grethe.ostby>

Fokus på sosio-tekniske scenarioer.



Takk for oppmerksomheten

Spørsmål